

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-215244

(43)Date of publication of application : 11.08.1998

(51)Int. Cl. H04L 9/14
H04L 9/36

(21)Application number : 09-012810 (71)Applicant : SONY CORP

(22)Date of filing : 27.01.1997 (72)Inventor : KUBOTA ICHIRO
ASANO TOMOYUKI

(30)Priority

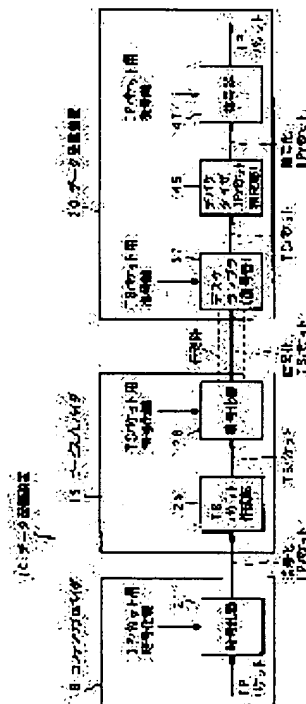
Priority number : 08316726 Priority date : 27.11.1996 Priority country : JP

(54) INFORMATION TRANSMITTER AND METHOD, INFORMATION RECEIVER AND METHOD, AND
INFORMATION STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide the information storage medium that stores digital data received through a data transmission channel from an information server together with a contents ID depending on a type of the data.

SOLUTION: A data distributor 10 applies duplicate encryption processing to digital data together with encryption processing using a cryptographic key depending on an identifier denoting a kind of the digital data and transmits the duplicate encryption data to a data receiver 30. The data receiver 30 receives the duplicate encryption data sent from the data distributor 10 through a satellite channel and applies decoding processing to the data by using respective decoding keys corresponding to the respective encryption keys.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision
of rejection][Kind of final disposal of application
other than the examiner's decision of
rejection or application converted
registration]

[Date of final disposal for application]

[Patent number]

BEST AVAILABLE COPY

[Date of registration]

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against
examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998, 2000 Japanese Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 1 0 - 2 1 5 2 4 4

(43) 公開日 平成 1 0 年 (1 9 9 8) 8 月 1 1 日

(51) Int. Cl. ⁹

H04L 9/14
9/36

識別記号

庁内整理番号

F I

H04L 9/00

641

685

技術表示箇所

審査請求 未請求 請求項の数 3 3 O L (全 1 8 頁)

(21) 出願番号 特願平 9 - 1 2 8 1 0

(22) 出願日 平成 9 年 (1 9 9 7) 1 月 2 7 日

(31) 優先権主張番号 特願平 8 - 3 1 6 7 2 6

(32) 優先日 平 8 (1 9 9 6) 1 1 月 2 7 日

(33) 優先権主張国 日本 (J P)

(71) 出願人 0 0 0 0 0 2 1 8 5

ソニー株式会社

東京都品川区北品川 6 丁目 7 番 3 5 号

(72) 発明者 窪田 二郎

東京都品川区北品川 6 丁目 7 番 3 5 号 ソ
ニー株式会社内

(72) 発明者 浅野 智之

東京都品川区北品川 6 丁目 7 番 3 5 号 ソ
ニー株式会社内

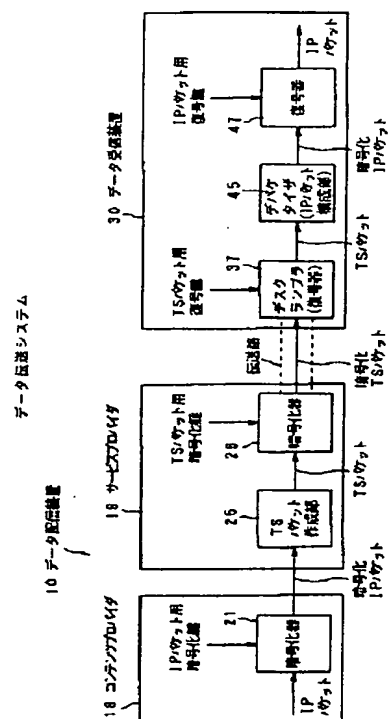
(74) 代理人 弁理士 小池 晃 (外 2 名)

(54) 【発明の名称】 情報伝送装置及び方法並びに情報受信装置及び方法並びに情報記憶媒体

(57) 【要約】

【課題】 通信衛星を用いるデータ伝送システムでは、不特定多数の受信装置での受信が可能であるので盗聴、妨害されやすい。

【解決手段】 データ配信装置 1 0 は、デジタルデータに該デジタルデータの種類の示す識別子に応じた暗号鍵を用いた暗号化処理を含め、2 重の暗号化処理を施し、この 2 重暗号化データを送信する。データ受信装置 3 0 は、データ配信装置 1 0 から衛星回線を介して送信された上記 2 重暗号化データを受信し、それぞれの暗号鍵に応じたそれぞれの復号鍵を用いて復号処理を施す。



【特許請求の範囲】

【請求項 1】 デジタルデータを所定のデータブロックに分割し、該データブロックをデータ伝送路を介して伝送する情報伝送装置において、

上記デジタルデータに上記デジタルデータの種類を示す識別子に応じた暗号鍵を用いた暗号化処理を含め、少なくとも 2 重の暗号化処理を施し、この暗号化データを送信する送信手段と、

上記送信手段から上記データ伝送路を介して送信された上記暗号化データを受信し、それぞれの暗号鍵に応じたそれぞれの復号鍵を用いて復号化処理を施す受信手段とを備えることを特徴とする情報伝送装置。

【請求項 2】 上記所定のデータブロックは、複数のシステム相互間でネットワークを介してデジタルデータの送受信を行うためのインターネットプロトコルによるパケットであることを特徴とする請求項 1 記載の情報伝送装置。

【請求項 3】 上記受信手段は、受信した上記暗号化データを全て復号化する前に、上記データを一時的に記憶手段に保存することを特徴とする請求項 1 記載の情報伝送装置。

【請求項 4】 上記データ伝送路とは別に、双方向のデータ伝送が可能な双方向データ伝送路を備えることを特徴とする請求項 1 記載の情報伝送装置。

【請求項 5】 上記データ伝送路として上記双方向データ伝送路よりも伝送容量の大きい衛星回線を用い、また上記双方向データ伝送路として地上通信網を用いることを特徴とする請求項 4 記載の情報伝送装置。

【請求項 6】 デジタルデータを所定のデータブロックに分割し、該データブロックをデータ伝送路を介して伝送する情報伝送方法において、

上記デジタルデータに上記デジタルデータの種類を示す識別子に応じた暗号鍵を用いた暗号化処理を含め、少なくとも 2 重の暗号化処理を施してからこの暗号化データを送信し、上記データ伝送路を介して受信した上記暗号化データにそれぞれの暗号鍵に応じたそれぞれの復号鍵を用いて復号化処理を施すことを特徴とする情報伝送方法。

【請求項 7】 上記所定のデータブロックは、複数のシステム相互間でネットワークを介してデジタルデータの送受信を行うためのインターネットプロトコルによるパケットであることを特徴とする請求項 6 記載の情報伝送方法。

【請求項 8】 受信した上記暗号化データを全て復号化する前に、上記データを一時的に記憶媒体に保存することを特徴とする請求項 6 記載の情報伝送方法。

【請求項 9】 上記データ伝送路とは別に、双方向のデータ伝送が可能な双方向データ伝送路を備えることを特徴とする請求項 6 記載の情報伝送方法。

【請求項 10】 上記データ伝送路として上記双方向デ

ータ伝送路よりも伝送容量の大きい衛星回線を用い、また上記双方向データ伝送路として地上通信網を用いることを特徴とする請求項 9 記載の情報伝送方法。

【請求項 11】 デジタルデータの種類を示す識別子に応じた暗号鍵を用いた暗号化処理が少なくとも施された暗号化データを記憶していることを特徴とする情報記憶媒体。

【請求項 12】 データの種類を示す識別子が付加された複数種類のデータブロックよりなる多重化データをデータ伝送路を介して受信する情報受信装置において、上記識別子を読み取り、予め登録された種類のデータブロックのみを抽出して復号することを特徴とする情報受信装置。

【請求項 13】 受信可能な種類のデータブロックの識別子をその識別子と対応する復号鍵と共に参照テーブルに持つことを特徴とする請求項 12 記載の情報受信装置。

【請求項 14】 暗号化された上記データブロックを受信したときには、上記参照テーブルを参照し、識別子に応じた復号鍵に基づいて復号処理を該暗号化データブロックに対して施すことを特徴とする請求項 13 記載の情報受信装置。

【請求項 15】 上記データブロックとして、複数のシステム相互間でネットワークを介してデジタルデータの送受信を行うためのインターネットプロトコルによるパケットを用いることを特徴とする請求項 12 記載の情報受信装置。

【請求項 16】 上記識別子として、複数のシステム相互間でネットワークを介してデジタルデータの送受信を行うためのインターネットプロトコルパケットのヘッダに含まれる送信先アドレスを用いることを特徴とする請求項 12 記載の情報受信装置。

【請求項 17】 上記識別子として、上記データブロックの情報の種類を表すコンテンツ ID を用いることを特徴とする請求項 12 記載の情報受信装置。

【請求項 18】 上記識別子を各データブロックの先頭に付加されたメディアアクセス制御ヘッダの中に持つことを特徴とする請求項 12 記載の情報受信装置。

【請求項 19】 上記各データブロックの先頭に付加された上記メディアアクセス制御ヘッダの中に上記識別子の種別を表すためのフラグを持つことを特徴とする請求項 18 記載の情報受信装置。

【請求項 20】 上記データ伝送路とは別に、双方向のデータ伝送が可能な双方向データ伝送路を備えることを特徴とする請求項 12 記載の情報受信装置。

【請求項 21】 上記データ伝送路として上記双方向データ伝送路よりも伝送容量の大きい衛星回線を用い、また上記双方向データ伝送路として地上通信網を用いることを特徴とする請求項 12 記載の情報受信装置。

【請求項 22】 データの種類を示す識別子が付加され

た複数種類のデータブロックよりなる多重化データをデータ伝送路を介して受信する情報受信方法において、上記識別子を読み取り、予め登録された種類のデータブロックのみを抽出して復号することを特徴とする情報受信方法。

【請求項 2 3】 受信可能な種類のデータブロックの識別子をその識別子と対応する復号鍵と共に参照テーブルに持つことを特徴とする請求項 2 2 記載の情報受信方法。

【請求項 2 4】 暗号化された上記データブロックを受信したときには、上記参照テーブルを参照し、識別子に応じた復号鍵に基づいて復号処理を該暗号化データブロックに対して施すことを特徴とする請求項 2 3 記載の情報受信方法。

【請求項 2 5】 上記データブロックとして、複数のシステム相互間でネットワークを介してデジタルデータの送受信を行うためのインターネットプロトコルによるパケットを用いることを特徴とする請求項 2 2 記載の情報受信方法。

【請求項 2 6】 上記識別子として、上記インターネットプロトコルパケットのヘッダに含まれる送信先アドレスを用いることを特徴とする請求項 2 2 記載の情報受信方法。

【請求項 2 7】 上記識別子として、上記データブロックの情報の種類を表すコンテンツ ID を用いることを特徴とする請求項 2 2 記載の情報受信方法。

【請求項 2 8】 上記識別子を各データブロックの先頭に付加されたメディアアクセス制御のヘッダの中に持つことを特徴とする請求項 2 2 記載の情報受信方法。

【請求項 2 9】 上記各データブロックの先頭に付加された上記メディアアクセス制御ヘッダの中に上記識別子の種別を表すためのフラグを持つことを特徴とする請求項 2 8 記載の情報受信方法。

【請求項 3 0】 上記データ伝送路とは別に、双方向のデータ伝送が可能な双方向データ伝送路を用いることを特徴とする請求項 2 2 記載の情報受信方法。

【請求項 3 1】 上記データ伝送路として上記双方向データ伝送路よりも伝送容量の大きい衛星回線を用い、また上記双方向データ伝送路として地上通信網を用いることを特徴とする請求項 3 0 記載の情報受信方法。

【請求項 3 2】 データブロックの情報の種類を示すコンテンツ ID が付加された複数種類のデータブロックを記憶することを特徴とする情報記憶媒体。

【請求項 3 3】 上記コンテンツ ID は、各データブロックの先頭に付加されたメディアアクセス制御ヘッダの中のフラグにより判別されることを特徴とする請求項 3 2 記載の情報記憶媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】 本発明は、例えば、通信衛星

を用いて、データ配信サービスを行うための情報伝送装置及び方法並びに情報受信装置及び方法並びに情報記憶媒体に関する。

【 0 0 0 2 】

【従来の技術】 公衆電話回線、専用回線などを用いてデータ伝送する場合又は通話する場合、伝送情報の漏洩を防止するため又は伝送情報に対する妨害に対して情報の信頼性を維持するため、平文のデータを暗号化して伝送し、受信先で暗号化されたデータを復号している。

【 0 0 0 3 】 代表的な暗号方式としては、共通鍵暗号方式と公開鍵暗号方式とが知られている。共通鍵暗号方式は対称暗号系とも呼ばれており、アルゴリズム非公開型とアルゴリズム公開型がある。アルゴリズム公開型の代表的なものとして、DES (Data Encryption Standard) が知られている。公開鍵暗号方式は、暗号化鍵から復号鍵を導出するために莫大な計算量が必要なため実質的に復号鍵が解読されないので、暗号化鍵を公開してもよい暗号方式であり、非対称鍵暗号方式ともよばれている。

【 0 0 0 4 】 図 1 7 は、伝送路上のデータを共通鍵暗号方式で暗号化する暗号化データ伝送装置の一例を示す概略構成図である。この暗号化データ伝送装置は、送信者側の送信装置 9 1 と、受信者側の受信装置 9 2 とをつなぐデータ伝送路 9 4 から盗聴者側の盗聴装置 9 3 がデータを盗聴するのを防ぐ。

【 0 0 0 5 】 伝送すべきデータには、送信装置 9 1 内の暗号化器 9 6 により暗号鍵 9 7 を用いての暗号化処理が施される。データ伝送路 9 4 により伝送されて受信装置 9 2 で受信された上記暗号化データは、復号鍵 9 8 を用いた復号器 9 9 により復号されて、復号データが得られる。

【 0 0 0 6 】 ここで、盗聴装置 9 3 がデータ伝送路 9 4 から受信装置 9 2 と同様に暗号化されたデータを受信しても、復号鍵 9 8 を持たないので、復号することが困難である。すなわち、盗聴装置 9 3 では、そのままでは意味不明の暗号化処理 (スクランブル) ののかかったデータを扱うことになるから、現実的に盗聴装置 9 3 側に情報が漏洩することを防ぐことができる。この例における共通鍵暗号方式の主要な暗号化方法では、一般に暗号化鍵と復号鍵は同一ビット列である。

【 0 0 0 7 】 なお、上述したような、暗号化方式は、伝送データが伝送される回線系統の種別、伝送データの機密度 (機密性)、伝送データの量などに応じて決定される。例えば、専用回線を用いたデータ伝送においては、情報の漏洩、伝送データへの妨害の度合いは低いが、公衆電話回線を用いてデータ伝送する場合は情報の漏洩の度合い、妨害の度合いは高くなる。

【 0 0 0 8 】

【発明が解決しようとする課題】 ところで、近年、通信衛星を用いたデジタルデータの伝送が可能になったこ

とで、テレビジョン放送や映画などのアナログ映像・音声データのみならず、コンピュータなどで利用されるテキストやデジタル映像・音声データについても、通信衛星を用いて伝送されるようになったが、不特定多数の受信装置での受信が可能であることから情報の漏洩の度合い、妨害の度合いは一層高くなる。

【0009】すなわち、上記通信衛星を用いるデータ伝送システムでは、電話回線、専用回線などの1対1通信と異なり、不特定多数の受信者が受信装置で容易に受信できるので、盗聴されやすい。このため、例えば有料のデータ伝送が盗聴される可能性が高い。そこで、上記データ伝送システムでも、データの暗号化が必要とされる。

【0010】実際の上記データ伝送システムにおいては、全てのデータについて暗号化処理を施すのではなく、送信装置において伝送すべきデータの内容に応じて、暗号化すべきデータを暗号化して伝送路上に送出し、受信者は暗号化されたデータの全部又は一部を復号して、その結果得られた情報により、或いは、暗号化されずに伝送された部分により、そのデータが自分にとって必要なものであるか否かを知る。

【0011】ここで、通信衛星を使った従来のテレビジョン放送サービスは、配信者が配信したデータを同時に多数のユーザが受信して使用する形態である。これに対して、コンピュータなどで使用されるデジタルデータを、通信衛星を介して配信する場合には、データ配信者から単数または複数の特定のユーザにデータを配信する機能が求められる。

【0012】しかし、従来、データ配信者から多ユーザへの同時通信又は放送システムでは、全ユーザは常に同じ情報を受信して使用又は閲覧をしており、システムユーザ個人の識別情報がないため、データ配信者から特定ユーザのみへのデータの配信ができなかった。

【0013】本発明は、上記実情に鑑みてなされたものであり、上記通信衛星を用いてデジタルデータを伝送する際にも、情報の漏洩の度合い、妨害の度合いを低くできる情報伝送装置及び方法の提供を目的とする。

【0014】また、本発明は、上記実情に鑑みてなされたものであり、情報配信者からデータ伝送路を介して伝送されたデジタルデータを、データの種類に応じて特定のユーザのみが受信できるようにする情報受信装置及び方法の提供を目的とする。

【0015】また、本発明は、上記実情に鑑みてなされたものであり、少なくとも情報送信者側でデジタルデータの識別子に応じた暗号鍵により、暗号化された暗号化データを記憶している情報記憶媒体の提供を目的とする。

【0016】また、本発明は、上記実情に鑑みてなされたものであり、情報配信者からデータ伝送路を介して伝送されたデジタルデータを、データの種類に応じたコ

ンテンツIDと共に、記憶している情報記憶媒体の提供を目的とする。

【0017】

【課題を解決するための手段】本発明に係る情報伝送装置及び方法は、上記課題を解決するために、上記デジタルデータに上記デジタルデータの種類の示す識別子に応じた暗号鍵を用いた暗号化処理を含めた少なくとも2重の暗号化処理を施してからこの暗号化データを送信し、データ伝送路を介して受信した上記暗号化データにそれぞれの暗号鍵に応じたそれぞれの復号鍵を用いて復号処理を施す。

【0018】また、本発明に係る情報記憶媒体は、上記課題を解決するために、デジタルデータの種類の示す識別子に応じた暗号鍵による暗号化処理が少なくとも施された暗号化データを記憶している。

【0019】また、本発明に係る情報受信装置及び方法は、上記課題を解決するために、データの種類の示す識別子が付加された複数種類のデータブロックをデータ伝送路を介して受信し、上記識別子を読み取り、予め登録された種類のデータブロックのみを抽出して復号する。

【0020】また、本発明に係る情報記憶媒体は、上記課題を解決するために、データブロックの情報の種類を示すコンテンツIDが付加された複数種類のデータブロックを記憶する。

【0021】

【発明の実施の形態】以下、本発明に係る情報伝送装置及び方法並びに情報受信装置及び方法並びに情報記憶媒体の実施の形態について図面を参照しながら説明する。この実施の形態は、デジタルデータを所定のデータブロックに分割し、該データブロックを衛星回線を介して伝送する図1のデータ伝送システムである。

【0022】このデータ伝送システムは、デジタルデータに上記デジタルデータの種類の示す識別子に応じた暗号鍵を用いた暗号化処理を含め、2重の暗号化処理を施し、この2重暗号化データを送信するデータ配信装置10と、このデータ配信装置10から上記衛星回線を介して送信された上記2重暗号化データを受信し、それぞれの暗号鍵に応じたそれぞれの復号鍵を用いて復号処理を施すデータ受信装置30とを備えてなる。ここで、データ受信装置30は、例えばパーソナルコンピュータの拡張スロットに装着される。なお、図1には、パーソナルコンピュータをそのままデータ受信装置30として示している。

【0023】データ配信装置10及びデータ受信装置30は、双方向の通信が可能な例えばISDNのような地上通信網を介して相互に通信が可能である。この地上通信網は、複数のシステム相互間でネットワークを介してデジタルデータの送受信を行うインターネットに接続されていてよい。また、通信衛星18による衛星回線は、上記地上通信網よりも伝送容量が大きい。

【0024】先ず、上記データ伝送システムにおけるデータの流れを説明する。ここでは、データ配信装置10を所有するデータ提供者とデータ受信装置30を所有する特定のユーザが、データの配送の契約を予め結んでいるものとする。なお、ここでいうデータ提供者とは、伝送情報を提供する事業者（以下、コンテンツプロバイダという）と、伝送路を提供する事業者（以下、サービスプロバイダという）の両方を含めている。

【0025】データ受信装置30を所有するユーザは、例えば、地上通信網としてのISDNを介して、データ提供者が提供する所定のサービスを受けたい旨のリクエストをデータ配信装置10に送る。このリクエストを送る方法は、特に、限定されず、データの種別やユーザとの契約状況によって決められ、例えば郵便などでもよい。また、リクエストを送らずに、予め契約に従って、データ提供者がサービスを提供してもよい。

【0026】データ配信装置10に送られたユーザからのリクエストは、データリクエスト受付部11で受け取られ、データ管理部12に送られる。データ管理部12は、ユーザの契約情報やリクエストが意味のあるものかのチェックを行い、問題が無ければ、データ蓄積部13にデータの読み出し要求を行う。データ蓄積部13は、データ読み出し要求に応じた、例えばデータを高速スイッチャ14を介してデータ作成部15に送る。

【0027】データ作成部15では、データ蓄積部13からのデータに対してIPパケット化、メディアアクセス制御(Media Access Control、MAC)フレーム化、MPEG(Moving Picture Experts Group Phase)2のトランスポート化などのフォーマット変換を行う。また、データ作成部15は、データのIPパケット化後と、トランスポート化後に、上記2重の暗号化を行う。

【0028】このフォーマット変換について以下に説明する。上述したように、近年、オーディオ、ビデオ信号やデータのような多種類のデータが多重化されて、大容量のデジタル回線で伝送されることが可能になってきた。この多重化の方法としては、例えばMPEG2の伝送フォーマットであるトランスポートストリーム(Transport Stream、TS)パケットが知られている。このTSパケットでは、情報データ部(ペイロード部)に暗号化処理を施している。この暗号化のための暗号化鍵は、TSパケットのヘッダ部分の13ビットのパケットID(PID)及び2ビットのスクランブル制御部に対応した固有のビット列を使用する。また、上記PIDは、各TSパケットの特定チャンネルのビデオやオーディオ等の情報種別を識別するのに使われる。

【0029】このTSパケットを用いてデータを伝送する場合には、データをインターネットで広く使用されているインターネットプロトコル(IP)パケットのフォーマットに変換し、さらにこのIPパケットをTSパケットに入れ込んでいる。

【0030】ところで、多種類のデータがIPパケットとして伝送される場合、上記PIDはIPパケットのデータを他のビデオやオーディオのデータと識別するために使われており、又ビット長も13ビットしか無く、IPパケットで伝送される種々のデータの種別を識別させるには不十分なビット数である。そこでPID以外のデータ種別の識別方法が必要になる。

【0031】例えば、インターネット上では受信データが自分宛のデータであるか否かを識別するのにIPパケットのIPヘッダに含まれる送信先アドレス(DestinationAddress)を用いている。TSパケットでIPパケットを伝送する場合でも、この送信先アドレス(以後、送信先IPアドレスという。)を用いて自分宛のデータであることを識別することが可能である。

【0032】しかし、例えば衛星回線を例にとるとデータ伝送速度が1中継器当たり30Mbpsとなり、データ受信側でリアルタイムに送信先IPアドレスの解析をソフトウェアで行うことは非常に困難である。何らかの手段により、自分宛の情報だけを抽出する手段が必要となる。

【0033】さらに、具体的な情報のタイトルを指定しなくとも、自分の関心のある情報のジャンルの情報だけ指定しておけば、そのジャンルの情報だけが自動的に受信され、ダウンロードできると大変便利である。

【0034】又、特定の加入者だけに受信可能とするために、上述したようにデータを暗号化した場合、受信側では暗号化されたデータを復号する必要がある。

【0035】そこで、上記データ伝送システムでは、データ配信装置10において複数種類のデータブロックからなる多重化データにデータの種別を示す識別子を付加し、通信衛星18を経由させて上記衛星回線により、データ受信装置30に送信している。そして、データ受信装置30では、ハードウェア的に上記識別子を読み取り、受信者が必要とする予め登録された種別のデータのみを抽出して復号する。

【0036】この識別子の付加は、データ配信装置10のデータ作成部15によって行われる。データ配信装置10内のデータ蓄積部13には、ユーザが必要とするデータが何も加工されていない状態で蓄積されている。データ管理部12から、データの読み出し要求がユーザから来たことを知らされたデータ蓄積部13は、リクエストされたデータ及びユーザの宛先情報を同時にデータ作成部15に高速スイッチャ14を介して送る。

【0037】ここで、ユーザの宛先情報とは、IPパケット送信に必要な送信先IPアドレスである。このデータ伝送システムでは、すべてのユーザに固有の送信先IPアドレスを割り振っている。一のユーザが持つ送信先IPアドレスは、一のユーザが確保している間は、一のユーザ以外のユーザは持たない。

【0038】データ蓄積部13からのデータは、データ

作成部 1 5 によって作成又はフォーマット変換された後、データ処理部 1 6 で他のオーディオ信号やビデオ信号と多重化され、多重化データとして送信アンテナ 1 7 から通信衛星 1 8 に無線回線を介して送られる。

【0039】通信衛星 1 8 を介して送られた多重化データは、特定ユーザの所有するデータ受信装置 3 0 に限らず、データを受信できる状況にある全てのユーザが受信することが可能である。データ受信装置 3 0 は、通信衛星 1 8 からの全多重化データを受信し、その中から、自分が出したリクエストに応じたデータを選別して抽出し、復号化する。

【0040】このデータ受信装置 3 0 は、データの種別を示す識別子が付加された複数種類のデータブロックよりなる多重化データを通信衛星 1 8 による衛星回線を介して受信し、上記識別子を読み取ることにより、予め登録された種類のデータブロックのみを抽出して復号する。

【0041】すなわち、データ受信装置 3 0 は、リクエストに応じて送信されたデータを含む多数のデータブロックを受信し、その中から、自分宛のデータブロック、自分が受け取るべきデータブロック、自分が受け取ることができるデータブロックを選別して抽出する。なお、予めユーザとデータ提供者との契約によって、ユーザが持つデータ受信装置 3 0 は決定されている。

【0042】したがって、通常であれば、ユーザが持つデータ受信装置 3 0 を用いて、他のユーザ宛の特有のデータを選別することができない。

【0043】しかし、通信衛星 1 8 を用いる上記データ伝送システムでは、電話回線、専用回線などの 1 対 1 通信と異なり、不特定多数の受信者が受信装置で容易に受信できるので、盗聴されやすい。すなわち、データ伝送が盗聴される可能性が高い。そこで、上記データ伝送システムでも、データの暗号化が必要とされる。

【0044】このため、データ配信装置 1 0 は、図 2 に簡単に示すように、情報を提供するコンテンツプロバイダ 1 8 と、その情報を伝送するサービスプロバイダ 1 9 とで、暗号化器 2 1 と、暗号化器 2 6 により 2 重の暗号化処理を施している。

【0045】このデータ配信装置 1 0 は、実際には、上述した図 1 に示すように構成されており、特に図 2 に示したコンテンツプロバイダ 1 8 と、サービスプロバイダ 1 9 の備える各部は、図 3 に示すようなデータ作成部 1 5 に含まれる。

【0046】データ蓄積部 1 3 から送られてきた特定ユーザ宛のデータ及び IP アドレスは送信先 IP パケット作成部 2 0 に送られる。IP パケット作成部 2 0 では、データ蓄積部 1 3 から送られてきたデータとその時点でユーザを特定する送信先 IP アドレスを用いて、図 4 に示す IP パケット 6 0 を生成する。この IP パケット 6 0 の大きさは TCP/IP (Transmission Control Pro

ocol/Internet Protocol) で規定され、ユーザがリクエストしたデータがその大きさを超える場合には、このデータは複数の IP パケットに分割されて次の暗号化器 2 1 に転送される。

【0047】ここで使用される IP パケット 6 0 の IP ヘッダには、図 5 に示すユーザの送信先 IP アドレス 7 4 と、送信元の IP アドレス 7 3 が入っている。ここで、送信先 IP アドレス 7 4 は、3 2 ビットである。

【0048】IP パケット作成部 2 0 で作成された IP パケット 6 0 は、暗号化器 2 1 に転送される。暗号化器 2 1 では、IP パケット 6 0 内の 3 2 ビットの上記送信先 IP アドレス 7 4 によって、宛先が特定のユーザであることを知り、その時点で既にデータ提供者と特定のユーザとの間のみで知り合う IP パケット用暗号化鍵によって IP パケット 6 0 全体を暗号化する。暗号化式としては、例えば DES (Data Encryption Standard) などが採用される。

【0049】この暗号化器 2 1 は、上記 3 2 ビットの送信先 IP アドレス 7 4 を用いた暗号化を行うので、IP パケットの暗号化による限定受信だけでも 2 の 3 2 乗 (=約 4 3 億) 個の範囲に受信者を分けることができる。

【0050】ここで、コンテンツプロバイダ 1 8 は、データ受信装置 3 0 に対して、伝送する IP パケットの送信先 IP アドレスと、暗号化 IP パケットを復号するための復号鍵を予め与えておく。そして、IP パケットのペイロード部分をこの復号鍵に対応する暗号鍵で暗号化し、サービスプロバイダ 1 9 に送る。

【0051】ただし、暗号化は、特定のユーザに対する全てのデータについて施す必要はなく、データの種別によっては暗号化が行われないこともある。暗号化が行われない場合には、IP パケット作成部 2 0 から MAC フレーム作成部 2 2 に直接 IP パケット 6 0 が転送される。

【0052】ここでは、暗号化が行われる場合について説明する。暗号化は通常 6 4 ビットの平文に対して行われ、暗号化すべき IP パケット 6 0 のデータ長が 6 4 ビットの倍数でない場合には、データの埋め合わせ、すなわち無効データのパディングを行うことで IP パケット 6 0 全体を 6 4 ビットの倍数にし、IP パケット 6 1 とする。

【0053】特定のユーザ用の IP パケット 6 1 が暗号化された IP パケット 6 2 は、MAC フレーム作成部 2 2 に転送される。MAC フレーム作成部 2 2 では、暗号化器 2 1 によって暗号化された IP パケット 6 2 に対して、MAC ヘッダ 7 0 を付加する。

【0054】この MAC ヘッダ 7 0 は、図 6 に示すように 8 ビットの SSID (Server System ID) と、2 4 ビットの UDB (User Depend Block) 1 と、3 2 ビットの UDB 2 の計 6 4 ビットで構成されている。特に、M

ACヘッダ70のUDB2には、上記IPヘッダ内に書かれた送信先IPアドレスと同様の送信先IPアドレスが書き込まれる。

【0055】上記IPヘッダ内の送信先IPアドレスは暗号化されており、受信装置側では暗号を復号しなければ送信先IPアドレスを知ることができないが、上記MACヘッダ70にそれと同じ送信先IPアドレスがあれば、受信側では単にハードウェア的にそれを読み出すことで、自分宛のデータブロックであるか否かを知ることができる。この送信先IPアドレスはIPパケット作成部20からMACフレーム作成部22に直接渡される。

【0056】なお、上記UDB1には、3ビットのPBL (Padding_Byte_Length) と、1ビットのCP (Control_Packet) と、1ビットのEN (Encrypted_or_Not) と、1ビットのPN (Protocol_Type Available_or_No) と、2ビットのReserveと、16ビットのプロトコル番号 (Protocol_Type) がセットされる。

【0057】この内、PBLは、パディングバイト長であり、暗号化の際に埋め合わせされた無効なデータの長さである。これは、暗号化されたIPパケットを受信したユーザが正規なデータ長を知るために必要となる。

【0058】また、CPは、IPパケットに、ユーザが必要なデータかシステム運用に必要な制御データが入っているかを識別するビットである。通常、ユーザがリクエストした際に受け取るべきMACフレーム63のCPは、制御データではなくデータが入っていることを示している。

【0059】ENは、IPパケットが暗号化器21によって暗号化されているか否かを示す制御ビットである。このビット情報によってユーザは受信したMACフレーム63を復号するかしないか決定する。PNは、Protocol_Typeエリアに有用な情報があるか否かを示す制御ビットである。

【0060】図3のMACフレーム作成部22では、以上の制御ビットをIPパケット62に付加している。ここで、UDB2には、上記送信先IPアドレスの他、IPパケットの情報の種類を表すコンテンツIDをセットしてもよい。このコンテンツIDについては後述する。UDB2にセットされたのが、上記送信先IPアドレスであるか上記コンテンツIDであるかを識別させるのが上記SSIDである。

【0061】MACフレーム作成部22で生成されたMACフレーム63には、CRC計算部23にて計算されたCRC (Cyclic Redundancy Checking、巡回冗長検査) が付加される。このようにデータ配信装置10側でCRCの計算を行うことで、データ受信装置30は、受信したMACフレームが正しく通信衛星18から伝送されているかを検査することができる。CRC計算部23において生成された16ビットのCRCは、MACフレーム63の最後に付加されている。

【0062】このMACフレーム63は、セクション作成部24に転送されてMPEG2で規定されるセクションに変換される。図4に示すように、MACフレーム63は、セクション (Sec) ヘッダ71の直後に付加され、プライベートセクション64と呼ばれる。

【0063】このセクションヘッダ71のフォーマットを図7 (A) に示す。セクションヘッダ71のフォーマットは、MPEG2によって、規定され、テーブル (ID) T₁₁、セクションシンクインディケータS₁₁、プライベートインディケータP₁₁、リザーブR₁₁、プライベートセクションレングスP₁₁を有する。ここで、プライベートセクションレングスP₁₁には、MACフレームのデータ長が入る。

【0064】セクション作成部24で作成されたプライベートセクション64は、トランスポートパケット作成部25に転送される。トランスポートパケット作成部25では、転送されたプライベートセクション64をトランスポートパケット65₁₁、65₁₂、・・・65_{1n}に分割する。

【0065】トランスポートパケット65₁₁、65₁₂、・・・65_{1n}は、それぞれ188バイトで構成されている。これらのトランスポートパケット65₁₁、65₁₂、・・・65_{1n}には、4バイトのTSヘッダが付加される。

【0066】例えばTSヘッダ72のフォーマットを図7 (B) に示す。TSヘッダ72は、シンクバイトS₁₁、トランスポートエラーインディケータT₁₁、ペイロードユニットスタートインディケータP₁₁、トランスポートブライオリティT₁₁、上記PID、上記スクランブル制御部 (トランスポートスクランブルコントロール) T₁₁、アダプティションフィールドコントロールA₁₁及びコンティニティカウンタC₁₁を有する。

【0067】トランスポートパケット65₁₁、65₁₂、・・・65_{1n}の1個分の大きさは、上述したように188バイトと規定されているので、一般的に、一つのセクション64を複数のトランスポートパケットに分割する必要がある。

【0068】ここで、通常、一つのセクションは184バイト (188バイトからヘッダ長の4バイトを引いたバイト数) の整数倍長とは限らないので、一つのセクション64を複数のトランスポートパケット65₁₁、65₁₂、・・・65_{1n}に分割する際には、図4に示すように、スタッフィングバイトを用いたデータの穴埋めを行う。すなわち、184バイトの倍数でない一つのセクションを複数のトランスポートパケットに分割した場合、最後のトランスポートパケットの余ったデータエリアに、全てのビットがスタッフィングされたスタッフィング領域を形成する。

【0069】トランスポートパケット作成部25で作成された各トランスポートパケットは、暗号化器26に供

給される。暗号化器 26 は、図 2 に示すように TS パケット用暗号化鍵を用いて、上記各トランスポートパケットのデータ部分に暗号化処理を施す。

【0070】サービスプロバイダ 19 は、データ受信装置 30 に対して、伝送する TS パケットの PID 部分とスクランブル制御部の値と、この TS パケットを復号する復号鍵を予め与えておく。そして、コンテンツプロバイダ 18 から与えられた暗号化 IP パケットを TS パケット化し、さらにこの TS パケットのペイロード部分を上記復号鍵に対応する暗号鍵で暗号化して、暗号化 TS

10 パケットを作成し、衛星回線に送信する。

【0071】ここで、暗号化のための暗号化鍵は、上述したように、図 7 の (b) に示した TS ヘッダの PID (13 ビット) とスクランブル制御部 (2 ビット) に対応した固有のビット列を使用する。このため、最大で 15 ビット分、4096 通りの限定ができる。

【0072】既に IP パケットの送信先 IP アドレスを用いて上述したように 2 の 32 乗個の範囲に受信者を分けることができているので、この TS パケットの暗号化を組み合わせると、さらにその 4096 倍の範囲に受信者を分けることができ、より細やかな限定受信方式を構成できる。

【0073】また、独立の暗号化を 2 重に行うことにより、盗聴者がいずれか一方の暗号を解読することに成功したとしても、もう一方の暗号を解読できなければ平文データを得ることはできないので、より安全性の高い限定受信方式を構成できる。

【0074】また、ここでは IP パケットの暗号化による限定受信方式と、TS パケットの暗号化による限定受信方式をそれぞれコンテンツプロバイダ 18 と、サービスプロバイダ 19 という別の事業者で行うので、他者とは独立の限定受信方式を構成できる。これは、伝送路を提供する事業者と、伝送データを提供する事業者が異なり、それぞれが独立にユーザと限定受信契約を結びたい場合に有効である。事業者間で暗号鍵に関する情報が漏れてしまう虞もない。

【0075】コンテンツプロバイダ 18 と、サービスプロバイダ 19 で 2 重の暗号化が施されたデータは、データ転送部 27 に転送された後、マルチプレクサ等のデータ処理部 16 に伝送される。データ処理部 16 では、上記トランスポートパケットを他のデジタル化されたビデオ、オーディオ信号と多重化した後、変調、増幅する。

【0076】ブロードキャストされた特定ユーザのためのデータは、ユーザ側の受信アンテナ 31 で受信され、特定のユーザのデータ受信装置 30 に転送される。

【0077】受信アンテナ 31 により受信された信号は、IF の信号に変換され、データ受信装置 30 に入力される。図 8 にこのデータ受信装置 30 のブロック図を示す。また、図 9 には、このデータ受信装置 30 で行わ

れる 2 重の復号処理のフローチャートを示す。

【0078】チューナ 33、A/D 変換器 34、復調器 35 及びデコーダ 36 からなるフロントエンド 32 に入力された信号は、ここでデジタル信号に変換され、QPSK 復調処理及び誤り訂正処理が施されて、ステップ S1 のように暗号化された TS パケットデータとして受信される。

【0079】この暗号化された TS パケットは、デスクランブラ 37 に供給される。デスクランブラ 37 は、上記暗号化された TS パケットデータに TS パケットレベルのデスクランブル処理を施す。この場合、デスクランブラ 37 は、上記暗号化 TS パケットデータのヘッダ部分から PID 部とスクランブル制御部の値を読みとり、この値に対応する TS パケット用復号鍵がサービスプロバイダ 19 から与えられているか否かをステップ S2 で判断し、与えられているならばステップ S3 でこの暗号化 TS パケットのペイロード部分をこの復号鍵により復号し、復号された TS パケットを出力する。ここで、復号鍵がサービスプロバイダ 19 から与えられていなければ、ステップ S7 で暗号化 TS パケットを破棄する。

【0080】ステップ S3 で復号された TS パケットは、デマルチプレクサ 38 に供給される。ここで、デマルチプレクサ 38 は、上記データ処理部 16 で上記 TS パケットデータと共に多重化されたオーディオデータとビデオデータを分割し、オーディオデータをオーディオデコーダ 39 に供給し、ビデオデータをビデオデコーダ 40 に供給する。オーディオデコーダ 39 は、アナログオーディオを出力し、ビデオデコーダ 40 は NTSC エンコーダ 41 を介してアナログビデオを出力する。残った TS パケットデータは、デパケタイザ 45 に供給される。

【0081】デパケタイザ 45 は、図 4 で示したプライベートセクション 64 のフォーマットを再生し、CRC の値を計算し、データが正しく受信されたか否かを判定する。そして、デパケタイザ 45 は、ステップ S4 で上記プライベートセクション 64 を IP パケット化し、図 10 に示すようなフォーマットデータ 75 に変換する。このフォーマットデータ 75 は、FIFO 46 を介してこの IP パケットを復号する復号器 47 に転送される。

【0082】復号器 47 では、フォーマットデータ 75 内の MAC ヘッダの図 6 に示した UDB2 にセットされた識別子、ここでは送信先 IP アドレスを取り出し、これに対応する IP パケット用復号鍵がコンテンツプロバイダ 18 から与えられているか否かをステップ S5 で判断し、与えられていれば、ステップ S6 で IP パケットのペイロード部分をこの復号鍵を用いて復号し、復号された IP パケットを出力する。ここで、復号鍵がコンテンツプロバイダ 18 から与えられていなければ、ステップ S7 で暗号化 IP パケットを破棄する。

【0083】復号鍵は、上記識別子に対応させて、デュアルポートラム（DPRAM）48内の図11に示す参照テーブル80に収納されている。

【0084】この参照テーブル80は、受信可能な種類のデータブロックの識別子をその識別子と対応する復号鍵と共に持っている。識別子としては4バイトを使っており、復号鍵としては8バイトを使っている。

【0085】図中、識別子としては上述したように、送信先IPアドレスを用いても、コンテンツIDを用いても良く、その識別は受信パケットのMACヘッダの中のSSIDで行う。又参照テーブル80の値の設定はDPRAM48への入力を持つCPU42により行われる。

【0086】復号器47は、上記図10のフォーマットで暗号化IPパケットデータを受信し、MACアドレス内のUDB2の識別子を取り出すと、DPRAM48にアクセスし、先頭アドレスから16バイトおきにテーブル80中の識別子を検索し、識別子の後の4バイトに格納されたマスクビットの内、“1”となっている識別子のビットに対して受信パケット中の識別子とテーブル中の識別子の一致検出を行う。

【0087】マスクビットがH“ffffffffff”となっていれば、受信したパケットのMACアドレス中の識別子とテーブル中の識別子の全ビットの一致を確認し、入力した識別子と同じ識別子がDPRAM48内にあるとし、その識別子に対応する復号鍵（図中セッションキー）を取り出し、それ以降のIPパケットの復号処理を行う。

【0088】予め登録された参照テーブル80中の識別子の最後には、ENDコードがストアされており、識別子を検索していき、ENDコードが検出された場合は、そこで検索を抜け出し、その受信パケットは受信せずにステップS7で示したようにこの復号器47で廃棄される。

【0089】識別子としては、上述したように、送信先IPアドレスの他、コンテンツID（またはジャンルID）を使う。すなわち、図6に示したMACヘッダ70のUDB2には、送信先IPアドレスの他、コンテンツIDがセットされてもよい。SSIDとして例えば“0”がセットされている場合には、送信先IPアドレスを用いることを示し、例えば“1”がセットされている場合には、ジャンルIDを用いることを規定する。SSIDを受信側で解析することによりどちらが使われているかを判別できる。

【0090】例えば、UDB2に送信先IPアドレスを用いた場合、ユニキャストアドレスに対応する個人宛、及びマルチキャストアドレスを用いてグループのユーザ宛のデータを伝送することが可能となり、受信側では自分宛かあるいは自分が所属しているグループ宛のデータのみリアルタイムで受信することが可能となる。

【0091】この場合、データ受信装置30のDPRAM

M48は図12に示すようなフォーマットの参照テーブル81を備えていればよい。この参照テーブル81は、受信可能な種類のデータブロックの送信先IPアドレスをその送信先IPアドレスと対応する復号鍵と共に持っている。例えば、始めの16バイトには上記マルチキャストアドレスのようなグループ用の送信先IPアドレス1がセットされている。

【0092】この送信先IPアドレス1の暗号化ON/OFFフラグは0である。また、次の16バイトには上記ユニキャストアドレスのような個人宛の送信先IPアドレス2がセットされている。暗号化ON/OFFフラグは1である。送信先IPアドレス2にもセッションキーがセットされている。

【0093】復号器47は、上記図10のフォーマットでIPパケットデータを受信し、MACアドレス内の送信先IPアドレスを入力すると、DPRAM48にアクセスし、先頭アドレスから16バイトおきにテーブル81中の送信先IPアドレスを検索し、該IPアドレスの後の4バイトに格納されたマスクビットの内、“1”となっている識別子のビットに対して受信パケット中の識別子とテーブル中の識別子の一致検出を行う。

【0094】マスクビットがH“ffffffffff”となっていれば、受信したパケットのMACアドレス中の送信先IPアドレスとテーブル中の送信先IPアドレスの全ビットの一致を確認し、入力したIPアドレスと同じIPアドレスがDPRAM48内にあるとし、そのIPアドレスに対応する復号鍵を取り出し、それ以降のIPパケットの復号処理を行う。

【0095】予め登録された参照テーブル81中のIPアドレスの最後には、ENDコードがストアされており、IPアドレスを検索していき、ENDコードが検出された場合は、そこで検索を抜け出し、その受信パケットは受信せずにこの復号器47でステップS7のように廃棄される。

【0096】一方、UDB2として32ビットをフルに使ったコンテンツIDを用いる場合は、予め登録しておいたジャンルのデータが受信された場合にデータをPCに転送し、ハードディスクに自動的にダウンロードすることが可能となる。

【0097】この場合、データ受信装置30のDPRAM48は図13に示すようなフォーマットの参照テーブル82を備えていればよい。この参照テーブル82は、受信可能な種類のデータブロックの例えばコンテンツID83を32ビットフルに使って、記憶している。

【0098】このような32ビットのコンテンツID83は、図14の（A）に示すように、8ビットの大分類D₁と、6ビットの中分類D₂と、4ビットの小分類D₃と、14ビットの情報IDとによって構成されている。大分類D₁は、コンピュータソフト、出版物、ゲームソフトというような大きなカテゴリーを表す。中分類D₂

は大分類D₁が出版物であれば、書籍、雑誌、新聞というような中間のカテゴリーを示す。さらに、小分類D₂は中分類D₁が新聞であれば、A新聞、B新聞、S新聞という新聞社名を表すカテゴリーを示す。そして、この小分類D₂の中の唯一のIDにより一つのデータ単位が識別される。この場合、新聞の発行の日付が情報IDとなり、結果的に例えば図14の(B)に示すようなコンテンツIDとなる。

【0099】このようなコンテンツIDを識別子として用いた場合の実際の情報識別の方法を以下に述べる。例えば、上記図14の例では、A新聞を契約する場合は、マスクビットをH“ffffc000”としてこのマスクビットが1のビット位置の受信パケットの識別子とテーブル中の識別子の一致を検出すればよい。また、固有の新聞名によらず、全ての新聞を受信する場合は、マスクビットをH“fffc0000”としておけば、A新聞H“02084000+発行日ID”、B新聞H“02088000+発行日ID”も全て一つの設定でダウンロードすることができる。

【0100】これは、いちいち個々の情報のIDを指定しなくても、必要な情報のジャンルだけ指定しておけば、自動的に指定したジャンルの情報が受信できる、という点で、大変有用な方法である。

【0101】ただこの場合、例えば各新聞が別々のセッションキーで暗号化されているように、各情報が暗号化されている場合は、コンテンツIDを設定するだけでは、各新聞に対するセッションキーを設定できないため、あくまでも各情報が暗号化されていない場合に有効な方法である。

【0102】なお、上記情報の識別子としては、48ビット長で各製品に割り当てられているMACアドレスを用いる方法もある。

【0103】復号器47で、送信先IPアドレスや、コンテンツIDを読むことが出来れば、このデータブロックが予め登録された種類のデータブロックであると判断して抽出し、フォーマットデータ75内の暗号化されたIPヘッダとIPデータを上述したように復号する。

【0104】復号化されたデータブロックは、パーソナルコンピュータ上のメインメモリにFIFO49及びPICインターフェース50を介して転送される。そして、このパーソナルコンピュータのソフトウェアによる処理がなされる。

【0105】CPU42は、DPRAM48の読み出しを制御すると共に、参照テーブルの値の設定を行う。また、CPU42は、ROM44からRAM43に読み込まれたプログラムにしたがって、デマルチプレクサ38、DPRAM48、DPRAM52を制御する。また、CPU42は、ICカードリーダー53から読み込んだデータを処理し、上記復号鍵を生成してもよい。また、上記リクエストをモデム54、及び電話回線56を

介してISDNによりデータ供給元に送信する。

【0106】以上説明したように、このデータ受信装置30は、データ配信装置10によりMACフレームのDBU2にセットされて伝送されてきた、送信先IPアドレスや、コンテンツIDを復号器47により読み取り、予め登録された種類のデータブロックのみを抽出することができるので、種々の暗号化されたデータが多重化された受信データの中から高速に、自分宛あるいは必要とする情報だけを抽出して復号できる。

【0107】また、伝送されたデータは、図2に示したように、コンテンツプロバイダ18、サービスプロバイダ19で2重に暗号化されており、データ受信装置30のみが、それを復号化する二つの復号鍵を持っていることから、データが他人に盗用されることを防止できる。

【0108】なお、この実施の形態となるデータ伝送システムは、データ配信装置10側の2重暗号化処理を図15に示すような構成で行ってもよい。すなわち、IPパケットの暗号化処理をコンテンツプロバイダ18に行わせるのではなく、サービスプロバイダ19に行わせる。このため、コンテンツプロバイダ18は、経費を節約できる。

【0109】すなわち、一つの事業者が両方の暗号化処理を行うように構成すれば、もう一方の事業者は暗号化処理のための設備を持つ必要がなくなる。これは、例えば一つのサービスプロバイダの提供する伝送路を複数のコンテンツプロバイダが利用する場合に、それぞれのコンテンツプロバイダが暗号化処理設備を持たなくてよいので有効である。

【0110】ここで各部の動作は、図2に示した各部の動作と同様であり、またデータ受信装置30の構成も同様であるので説明を省略する。

【0111】また、データ受信装置30内の構成を図16に示すようにしてもよい。すなわち、デバタイザ45と復号器47との間に例えばハードディスクドライバのような記憶装置58を設け、暗号化されたIPパケットを蓄積しておく構成としてもよい。このようにすれば、予めIPパケットを復号する復号鍵を得ていなくても、暗号化されたIPパケットを記憶装置58に蓄積しておいて、後から上記復号鍵を得た時点で復号すればよい。

【0112】すなわち、暗号化されたパケットを記憶装置に保存しておくようにすることにより、受信装置が復号鍵を後から得てもデータが有効となるようにできる。例えば、予め大量のデータを記憶装置に保存しておき、ユーザが意図した段階で復号鍵を得てデータを利用することにより、ユーザが意図してからデータを受信し始めるのに比べて、大量のデータを受信するための時間が節約できる。

【0113】ここでは、受信装置30がIPパケットを復号するための復号鍵を得ていない場合を説明したが、

T S パケットを復号するための復号鍵を得ていない場合でも、暗号化されたままの T S パケットを記憶装置に保存しておくことにより同様の処理を行える。

【0114】さらに、暗号化されたデータは、保存できるが、復号されたデータや復号鍵は保存できないような仕組みを付け加えることにより、平文データがコピーされることを防ぐことも可能になる。

【0115】また、上述した各例では、伝送データとして I P パケットを考えたが、同様の構造を持つ他の伝送プロトコルパケットを考えても、同様の限定受信方式が構成可能である。また、伝送データのパケット化を 3 重以上として、3 つ以上の限定受信方式を組み合わせてもよい。このため、I P パケット化前のファイルデータに暗号化処理を施しておいてもよい。

【0116】また、例えば、MAC フレームのデータ圧縮方法は、M P E G 2 には限定されず、他の圧縮方法を用いてよい。また、インターネットプロトコルは、T C P / I P には限定されず、例えば O S I (Open System Interconnection) 方式を用いてもよい。

【0117】

【発明の効果】本発明に係る情報伝送装置及び方法は、上記デジタルデータに上記デジタルデータの種類を示す識別子に応じた暗号鍵を用いた暗号化処理を含めた少なくとも 2 重の暗号化処理を施してからこの暗号化データを送信し、データ伝送路を介して受信した上記暗号化データにそれぞれの暗号鍵に応じたそれぞれの復号鍵を用いて復号処理を施すので、通信衛星を用いてデジタルデータを伝送する際にも、情報の漏洩の度合い、妨害の度合いを低くできる。

【0118】また、本発明に係る情報受信装置及び方法は、データの種類の示す識別子が付加された複数種類のデータブロックをデータ伝送路を介して受信し、上記識別子を読み取り、予め登録された種類のデータブロックのみを抽出して復号するので、情報配信者からデータ伝送路を介して伝送されたデジタルデータを、高速にデータの種類に応じて特定のユーザに受信させることができる。

【0119】また、本発明に係る情報記憶媒体は、デジタルデータの種類の示す識別子に応じた暗号鍵による暗号化処理が少なくとも施された暗号化データを記憶しているので、受信装置が復号鍵を後から得てもデータを有効に利用できる。

【0120】さらに、本発明に係る情報記憶媒体は、データブロックの種類を示すコンテンツ I D が付加された

複数種類のデータブロックを記憶するので、必要とする情報だけを簡単に抽出することができる。

【図面の簡単な説明】

【図 1】本発明の実施の形態となるデータ伝送システムの構成図である。

【図 2】上記データ伝送システムの 2 重暗号化処理に関わる構成を簡単に示したブロック図である。

【図 3】上記図 1 に示したデータ作成部の構成を示すブロック図である。

【図 4】上記図 3 に示したデータ作成部でのデータ作成の過程を説明するための図である。

【図 5】I P ヘッダの詳細な構成を示すフォーマット図である。

【図 6】MAC ヘッダのフォーマット図である。

【図 7】セクションヘッダと T S ヘッダのフォーマット図である。

【図 8】上記データ伝送システムを構成するデータ受信装置のブロック図である。

【図 9】上記データ受信装置で行う復号化処理を説明するためのフローチャートである。

【図 10】上記データ受信装置内のデパケタイザから復号器へのデータの転送を説明するための図である。

【図 11】上記データ受信装置内の D P R A M が格納する参照テーブルの基本的な構成図である。

【図 12】上記参照テーブルの第 1 の具体例を示す図である。

【図 13】上記参照テーブルの第 2 の具体例を示す図である。

【図 14】コンテンツ I D の具体的構成例を示す図である。

【図 15】上記データ伝送システム内のデータ配信装置の他の具体例を示すブロック図である。

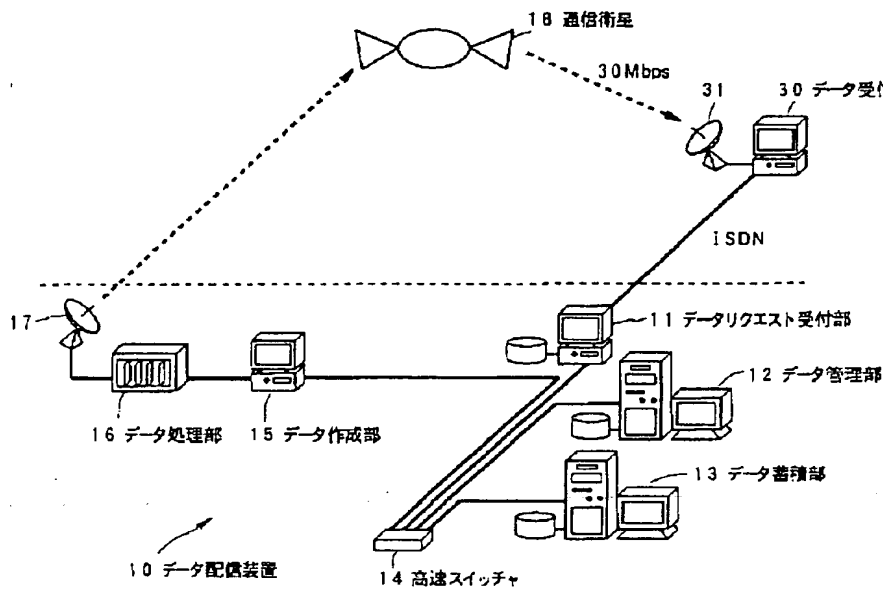
【図 16】上記データ伝送システム内のデータ受信装置の他の具体例を示すブロック図である。

【図 17】伝送路上のデータを共通鍵暗号方式で暗号化する暗号化データ伝送装置の一例を示す概略構成図である。

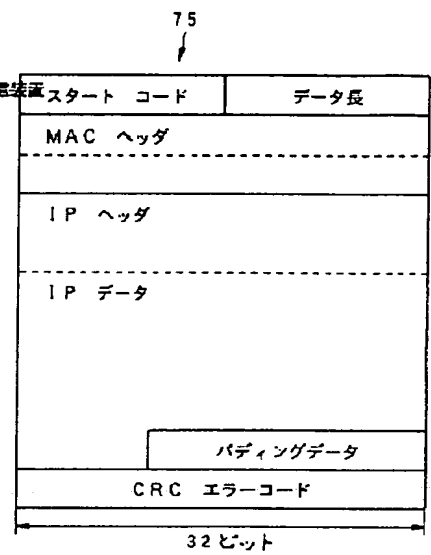
【符号の説明】

10 データ配信装置、18 コンテンツプロバイダ、
19 サービスプロバイダ、21 暗号化器、25 T
S パケット作成部、26 暗号化器、30 データ受信
装置、37 デスクランブラ、45 デパケタイザ、4
7 復号器

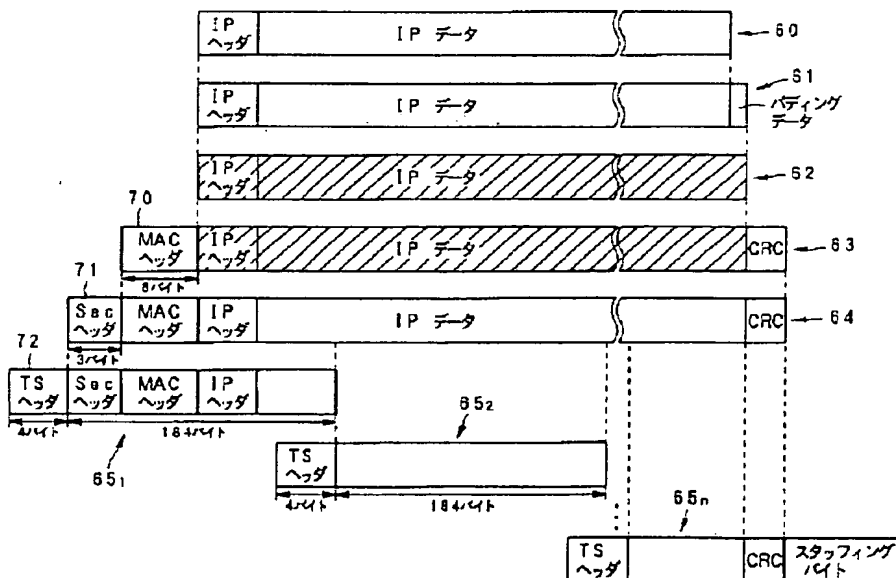
【図 1】



【図 10】

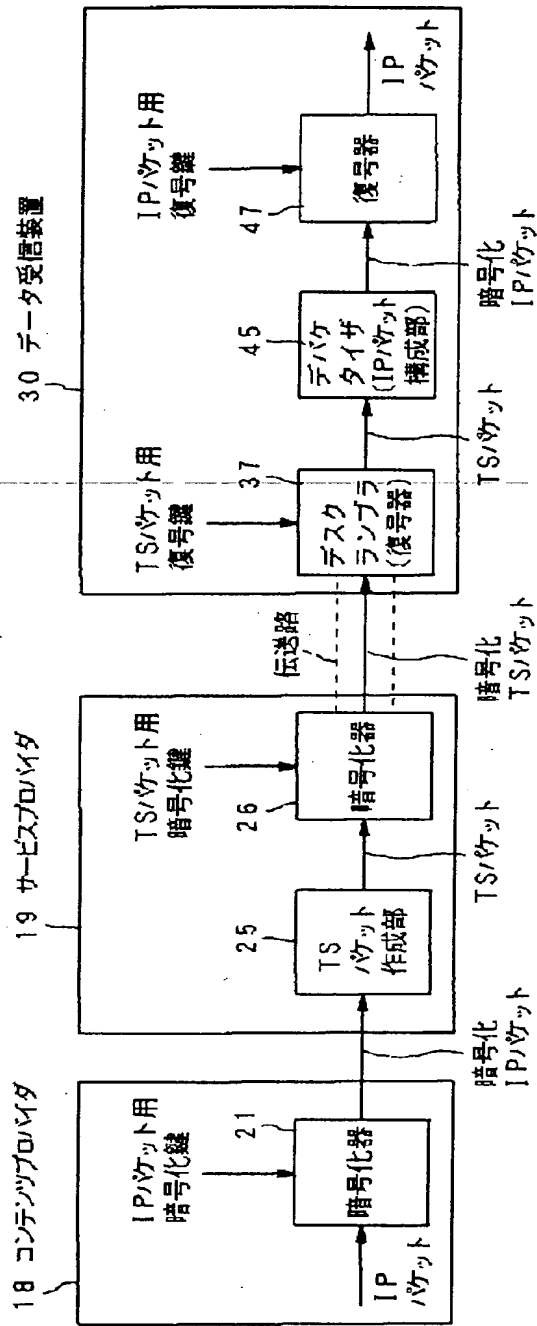


【図 4】



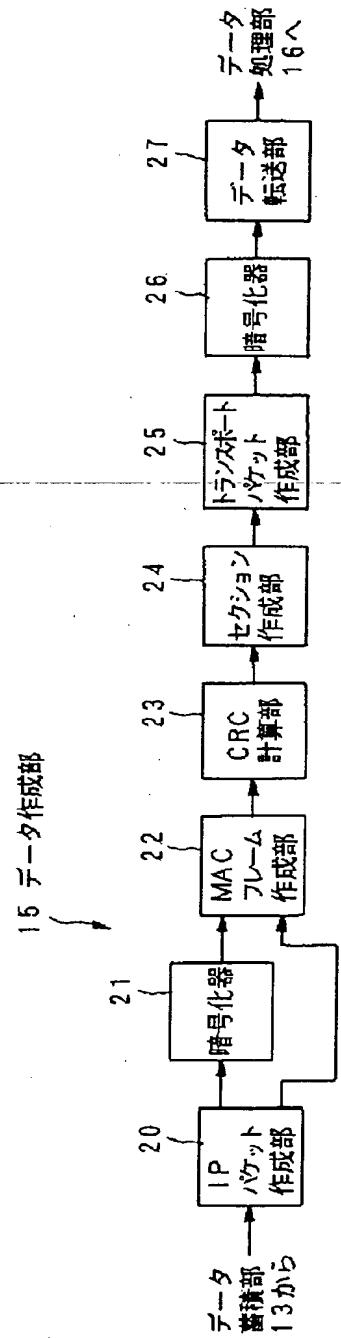
データ伝送システム

10 データ配信装置

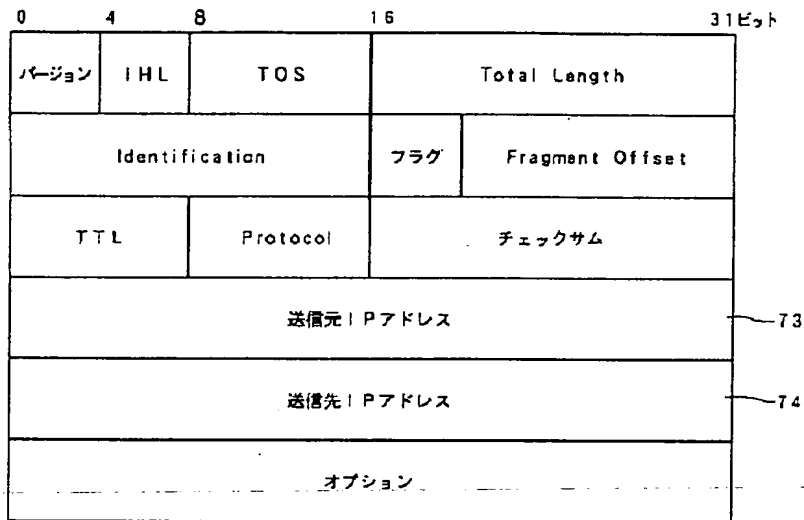


【図2】

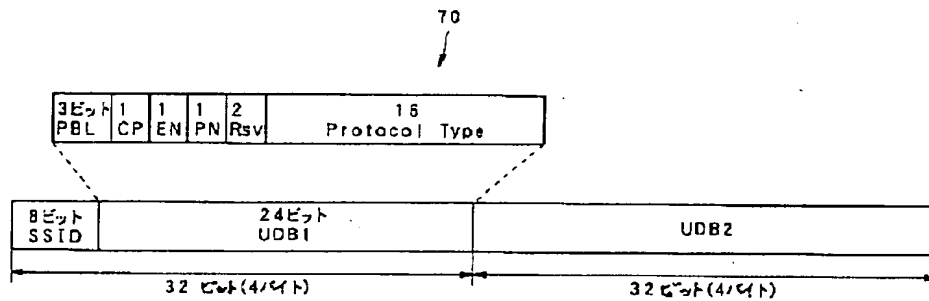
【図3】



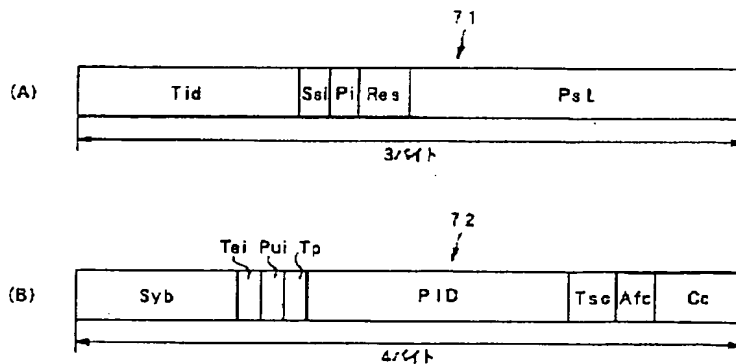
【図 5】



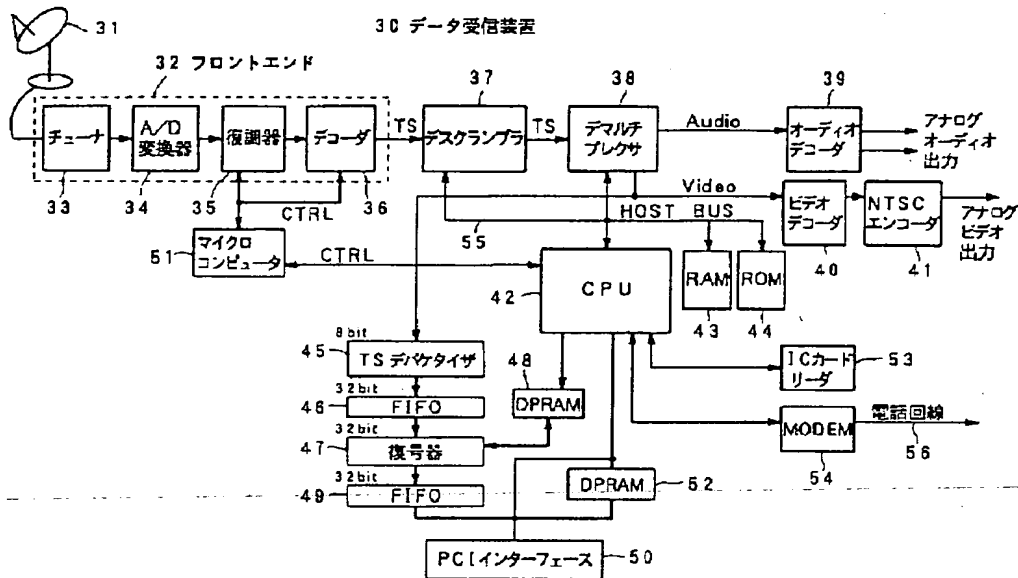
【図 6】



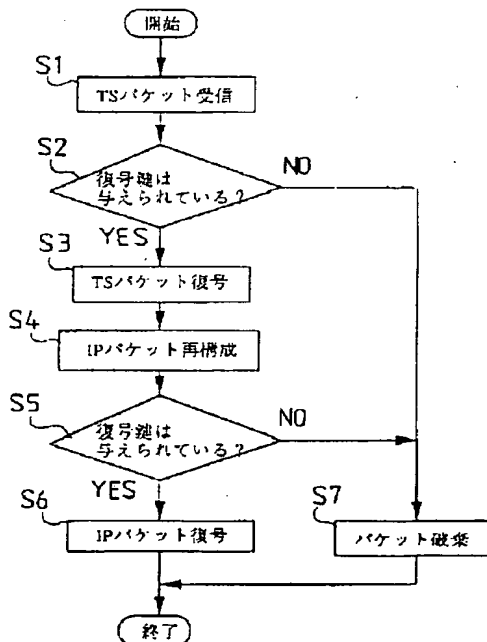
【図 7】



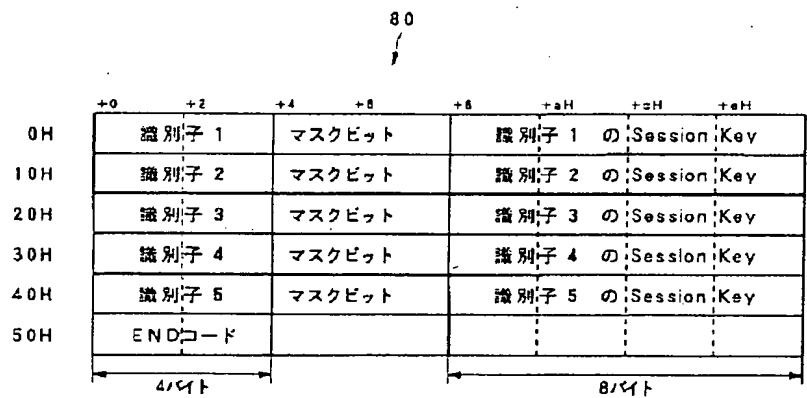
【図 8】



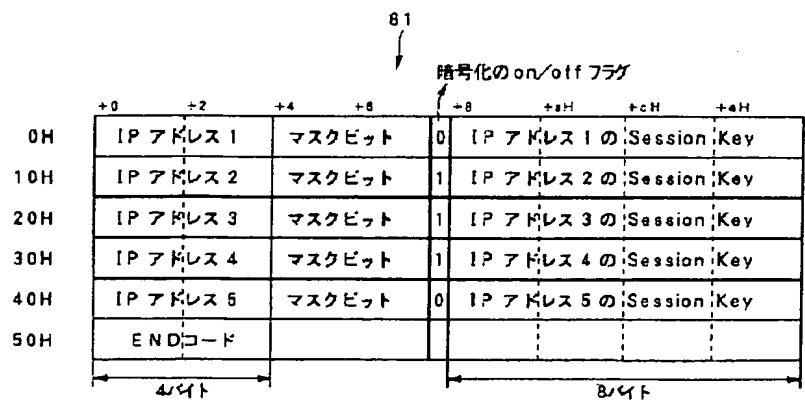
【図 9】



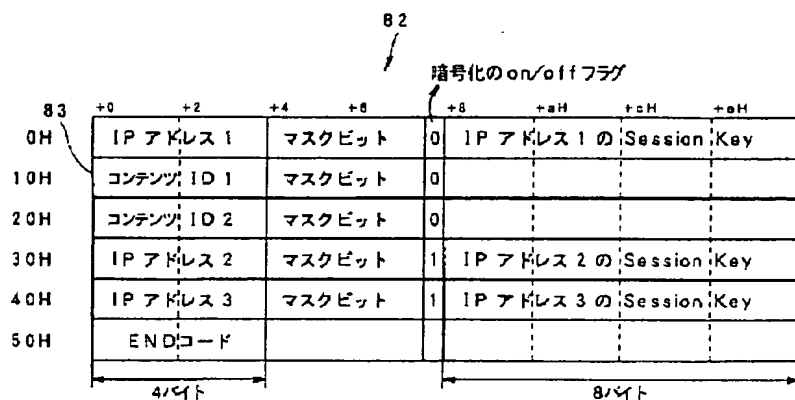
【図 11】



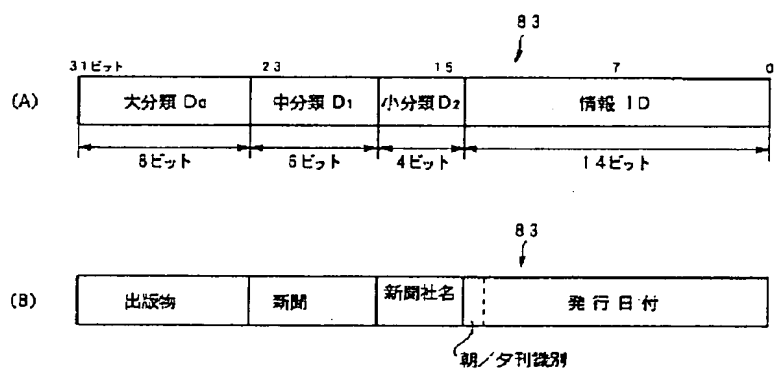
【図 12】



【図 13】

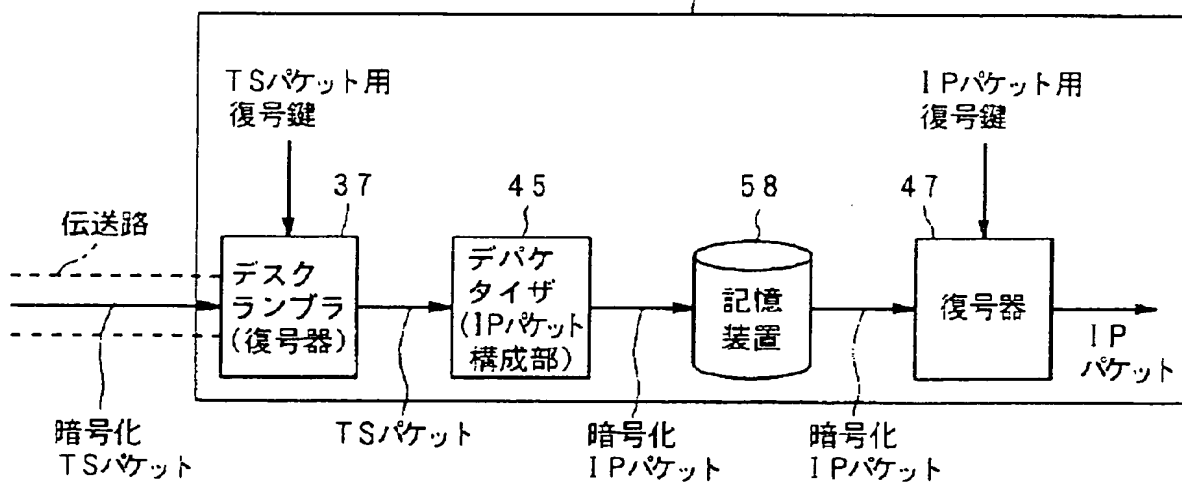


【図 14】

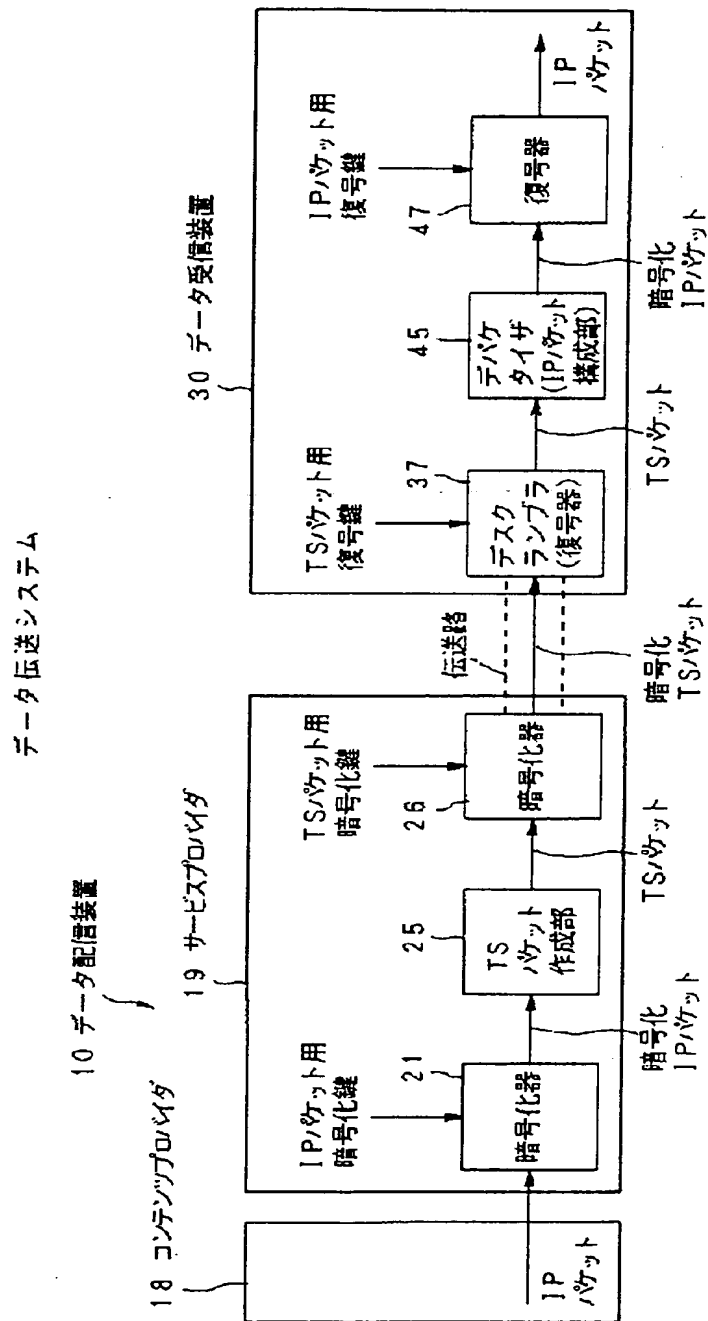


【図 16】

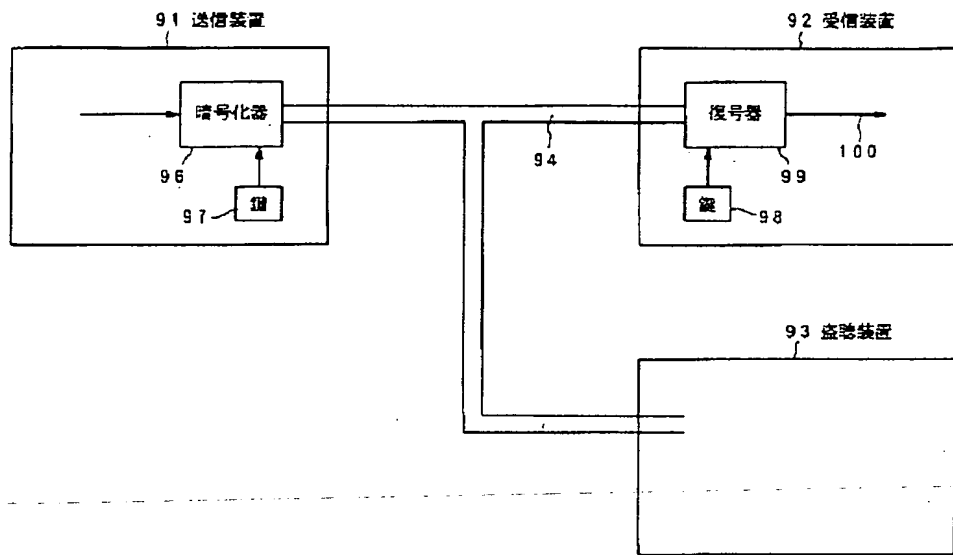
30 データ受信装置



【図 15】



【 図 1 7 】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.